BYTEWORKS

NETWORK SECURITY MANAGEMENT

Best Practices

All It Takes Is One Mistake

Suddenly, people all across your company find themselves locked out of their critical files. Your organization grinds to a halt. You've fallen victim to a ransomware attack—one of the most common and constantly evolving cyber threats of the past decade.

As IT manager, you take charge of the situation. You assess the damage, contact law enforcement, and begin implementing a data recovery plan from your last backup—but all the same, your organization has been effectively shut down, hopefully only temporarily. Or maybe you find that customers' and clients' sensitive data has leaked in a massive data breach that puts their trust in you in jeopardy or even fines from regulatory bodies. Ransomware and data breaches are two of the most costly cyberattacks—in terms of not only monetary loss and downtime, but in reputation as well.

Ask yourself—Is your organization safe enough from cybersecurity threats?

Cybersecurity Threats Are Evolving on a Daily Basis

Cyberattack attempts per week in 2021 increased by 50% compared with 2020, with the education and research sector, followed closely by government and military communications, seeing the largest jump in average weekly attacks per organization per industry. Yearly trends show that the number of cyberattacks are likely to increase through the end of 2022 and beyond.

With cybercriminals constantly devising new attack strategies and new twists on old phishing methods, keeping up-to-date on the best practices for network security is critical to ensuring as best as possible that your organization will continue to run smoothly and safely. There's no silver bullet for preventing all cyber-attacks forever—the best you can do is keep up to date with as many best practices as your IT department has the resources and executive buy-in to follow, with each best practice being a layer in your organization's cyber armor.

With the right focus on security, you can make your organization as safe as possible from cyber criminals, and if you ever do fall victim to a cyberattack, you can mitigate the damage and stave off the worst consequences of cyber crime.

Take Stock of Your IT Department's Swiss Cheese Cyber Defense Barrier

First coined in 1990 by James T. Reason of the University of Manchester, the Swiss cheese model of accident causation provides a model of computer security that is still widely used today. Think of every best practice for network security management as being a slice of Swiss cheese—every slice is full of holes, but as long as the holes don't happen to line up, a cyber threat getting through one hole still isn't likely to get all the way through.

As you read on, you can think of each of the following best practices as a slice of Swis-cheese. We'll group these slices into three categories based on the three layers of network security.

You'll probably find that you're already following some of the best practices—so especially take note of the ones you could be following but aren't, and what resources you would need to add them to your Swiss cheese cyber defense barrier if necessary.

Think of this list as a checklist to zero in on what you can do as an IT manager to better protect your company.

Three Layers of Network Security

The following network security checklist is divided into three sections, each focused on one of the three layers of network security:

Physical Network Security

This is the hardware layer—your actual physical IT equipment and network devices, and how you prevent unauthorized people from accessing them.

Technical Network Security

This is the software layer—the ways you manage and protect the flow of data across your network.

Administrative Network Security

This is the wetware layer—how you manage user behavior within your company through security policies and compliance processes.

Best Practices For Physical Network Security

Hollywood and television like to depict hackers as capable of performing nigh-supernatural acts with just a keyboard, but you know better.

Did you know, though, that many cyber threats such as data exfiltration happen simply because somebody could walk into your office and go somewhere they shouldn't have been able to get to?

One line of defense that can sometimes be overlooked is the actual physical hardware itself.

Prevent physical access by unauthorized persons to your routers, firewalls, and servers.

Make sure your company's network router is in a physically secure location—one that can only be accessed by your IT personnel for good cause: a locked room or closet, for example, rather than out in the open.

Never stick with default passwords for network devices.

Many companies will stick with the default network user IDs such as "admin" or "sysadmin" and passwords that come with their network devices out-of-the-box. Cybercriminals are well aware of this, and attempting to exploit it will usually be the first way of ingress they will attempt.

Make sure your network name, user IDs, and password are set to something unique rather than generic, especially something that might obfuscate whether the router is your company's network router to an outsider.

Consider security cameras or CCTV monitoring.

If your company handles extremely sensitive data, having security cameras trained on your network router, firewall, or server room is a smart idea for covering your bases—that way, you can detect unauthorized access to your IT equipment.

Having keycard or even biometric locks to your server room or your workplace as a whole is also a powerful method for securing your hardware and preventing unauthorized entry.

Best Practices for Technical Network Security

Your hardware is secure—now what about your software?

Perform thorough, regular network audits.

A network audit will help you identify weaknesses in your current network design and holes in your cyber armor that need covering. When you perform a network audit, you'll pick up on the presence of security vulnerabilities, open ports, and the status of your backups.

Looking into the status of your antivirus and anti-malware software and taking note of unused or unnecessary applications—noting that out-of-date applications especially can be vulnerable to security exploits—is another important facet of network audits.

When you perform an audit of your network, it can help to bring in a third-party vendor to assess the network. With fresh eyes, they can identify additional security gaps.

Make sure your antivirus and anti-malware software is up-to-date.

Antivirus, anti-malware, and malicious traffic detection software is in a constant arms race against viruses, malware, and hacker exploits. When these software tools are left to go without updates, you lose the arms race and allow new cyber threats to take you by surprise.

Use network and security tools such as firewall, SIEM, and DLP software.

Intrusion detection and prevention systems (IDS/IPS) are incredibly useful tools for preventing intrusions into your network traffic. One such IDS/IPS system is the firewall.

A physical firewall and web application firewall will protect your network and your website from web-based attacks, such as cross-site scripting and SQL injection attacks, the latter of which is one of the most common forms of web attacks.

Using a wide variety of network and security systems in tandem with your firewall, such as security information and event management (SIEM) systems, which act as a watchdog for your network and identify signs of intrusion such as impossible travel, excessive file copying, and file integrity changes.

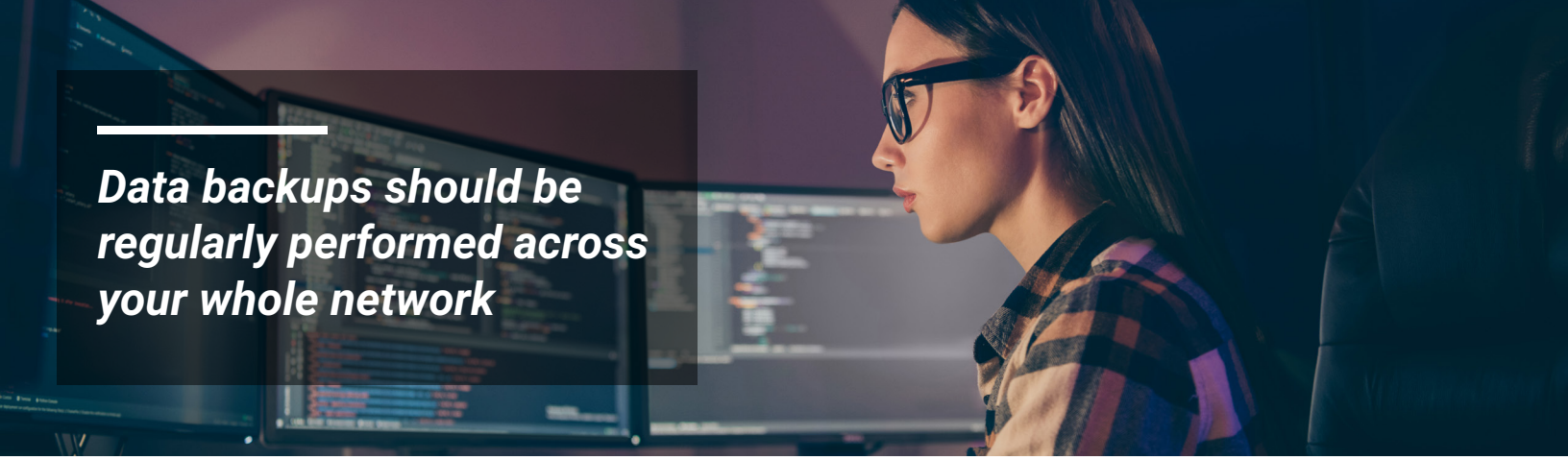
Data loss prevention (DLP) software is also crucial for network security, especially if your organization handles sensitive data. DLP software performs content analysis techniques such as database fingerprinting, exact file matching, and partial document matching to prevent the accidental loss and deletion of important files on your network.

Assign private IP addresses to critical devices and servers on the network.

Using private IP addresses for the critical devices and servers on your network is an important technique for preventing unauthorized attempts to access data. As an IT administrator, you can easily pinpoint unauthorized access attempts or suspicious activity by monitoring your network's private IP addresses.

Practice network segregation and segmentation.

When everything is fully connected, an intrusion into one department in your company becomes an intrusion into the entire company. When you segment and divide your organization's network into various trust zones, often segregated by department, you keep the networks relatively isolated so that a breach of one network will not lead to a breach of the entire organization. This method will greatly reduce the risks and impact of network intrusions.



Back up your data and ensure a recovery plan.

Backing up your data seems like common sense, but how effective is your backup plan? Many companies believe their backups are much more robust or readily available than they turn out to be when disaster hits.

With ransomware remaining one of the biggest threats to your organization's data, being able to restore the data you've lost without suffering the onerous cost of paying the hackers' ransom is critical to resuming operations swiftly, maintaining your customers' and clients' trust, and preventing financial hardship.

Data backups should be regularly performed across your whole network to ensure that whenever data loss ensues for any reason, you have relatively recent versions of the lost data ready to fill the holes. The older your backups are, the more out-of-date they are, the less useful they are, and the more hard work goes down the drain when you lose data.

You should have a recovery plan designed to get the backups in place and restore the lost data as soon as humanly possible to mitigate business disruption. Your plan should also take into account how long it takes to restore from a backup.

One rule of thumb for data backups you should keep in mind is the rule of three:

For a truly robust backup system, have three copies of your files—one in the cloud, one onsite, and one off-site. This will keep your data safe not only in the event of ransomware or other malware attacks but in case of hardware failure or natural disasters.

Audit your backup system regularly to ensure that the backups you have are truly useful enough to give your organization peace of mind.

Encrypt your sensitive data.

Hackers can't make use of your company's sensitive data if they can't read any of it. Especially when you have sensitive customer or client information such as credit card and other billing information, social security information, or data protected by regulatory standards such as HIPAA, making sure traffic to and from your organization's network is properly encrypted is crucial.

Employ VPNs for remote access to sensitive files.

Using a virtual private network (VPN) is critical for keeping your data encrypted as it passes in and out of your network, especially when one of your users is connecting to your network through a public connection. By encrypting data through the VPN, you prevent anybody from intercepting data entering and leaving the network.

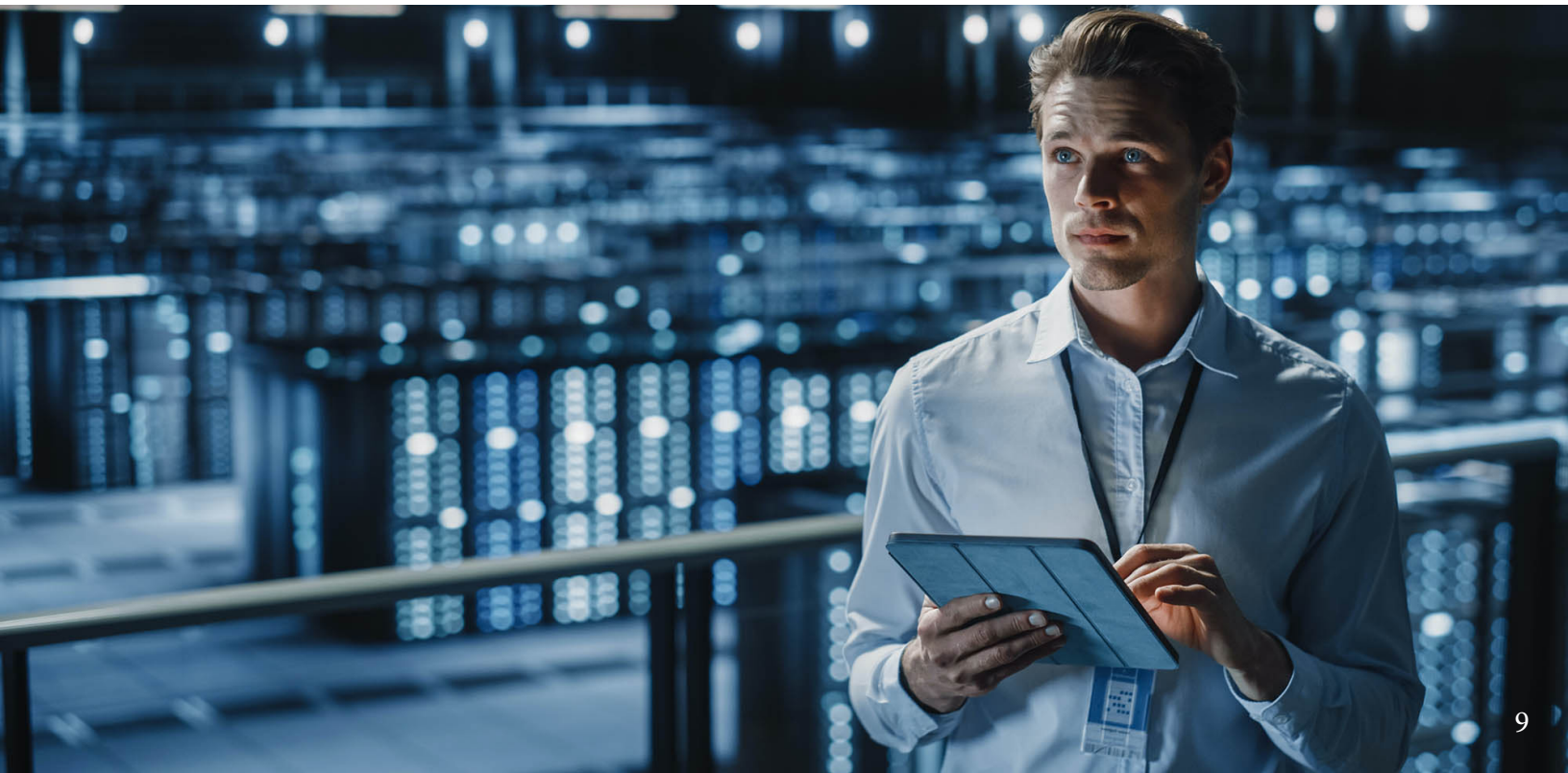
VPNs have seen a massive surge in use since the pandemic, when work-from-home—and work-from-anywhere—transformed how we work. Staff logging onto your network through a cafe's public Internet connection, for example, should always be logged into a VPN to encrypt their traffic.

In the past, VPNs were the domain of larger companies—their price points weren't economical for small businesses and organizations, especially not for high-speed networks. All that has changed, though, and VPN services for small businesses today are comparatively plentiful and cheap.

Disable file-sharing features for employee devices.

File-sharing tools, many of which are based in the cloud, are convenient for exchanging files between staff, but they are also fraught with risk. If file-sharing is a necessary function for your organization, use a secure, business-grade file-sharing platform.

Allow native file-sharing capabilities only on independent and private servers within your network and disable it on employee devices. Any file-sharing platform you employ should be easy for your IT security team to monitor.



Best Practices for Administrative Network security:

Last but not least in this best practices checklist, after hardware and software, is wetware.

Your organization's people are often the weakest link for cybercriminals to exploit. Phishing and other forms of social engineering are actually the most powerful and effective forms of cyberattack.

You can have all the physical and technical security the world can possibly offer—but one employee falling for a phishing email can make it all for naught.

Create a security-centered culture and communicate security policies.

For your network to be truly secure, everybody, not just you and your IT team, need to be well-versed in the ins and outs of a robust, secure network. Your entire staff must receive training on the importance of network security and understand the risks that come with a lack of security for your entire organization.

Clearly outline the requirements and expectations you have for IT security for new staff and third parties during the onboarding process, such as by including them in employment contracts, to ensure that everybody is well aware of what's expected of them from the very beginning.

Regularly educate your users on proper security hygiene.

Don't ever assume that everybody knows the basics of cybersecurity. As part of your organization's security culture, your staff will need to be regularly trained to follow proper security hygiene.

Phishing attacks are the most preferred methodology of most cyberattackers today, because they can easily take advantage of somebody who isn't fully paying attention to the emails that end up in their inboxes, and cybercriminals work hard to fool inattentive or under attentive end users into giving away sensitive information or inadvertently opening a backdoor into your network.

At the bare minimum, everybody in your organization should know:

- How to recognize a phishing email
- How to create and maintain strong, unique passwords
- Which applications are potentially dangerous
- Your organization's data protection policies, procedures, and regulations

Your security education should also remind users:

- Only use their work email for work communications
- Not to overshare on social media—cybercriminals will often stalk an organization's staff on social media to discern how users would answer security questions to access their accounts
- Not to auto-forward emails from their work accounts to their personal accounts while on vacation
- How to respond to ransomware attacks (by immediately disconnecting their device from the internet and intranet to limit the spread of the virus through the network)
- How to respond to a computer virus (i.e. to avoid backing up any files until the virus has been removed from their systems)

Because cyber threats are constantly evolving, user education must be an ongoing affair, not a one-and-done lesson. One useful method to build up your end users' network security skills is to stage fake phishing email campaigns to random employees, seeing who correctly avoids them and who falls for them.

Your network should take a "trust, but verify" approach to security

Build zero-trust architecture.

Trust, unfortunately, is hard to come by in the IT security world. Your network should take a "trust, but verify" approach to security and assume that cyber threatscan just as easily come from inside as they can from outside—because the sad reality of phishing and social engineering is that any one of your users can inadvertently become a threat from just a moment's carelessness.

User authentication, access management, multi-factor authentication, endpoint protection, and micro-segmentation are all components of a zero-trust security system. If you've been following all of these tips so far, you're already well on your way to creating a zero-trust system.

Multi-factor authentication forces your users to use something else, such as an authentication app on their phone or a text message, to log onto a platform or network in addition to their password. This ensures that even if their password is compromised, a bad actor cannot gain access to their systems.

Role-based access controls, which make it so that only certain users can use certain systems, are also important for making sure that a cyber Trojan horse (figurative or literal) cannot sneak itself into your network.

Endpoint security ensures that only certain devices (including computers, printers, scanners, other office equipment, and Internet-of-things devices) can connect to your network. Securing Internet-of-things (IoT) devices is especially crucial, as the use of IoT devices in business applications is growing and any device exposed to the internet is vulnerable to bot networks.

To secure your organization's IoT devices, be sure to automatically segment the devices using your organization's firewall policy and use IPS technologies to prevent exploits of known vulnerable devices.

Closely related to endpoint security, mobile device management (MDM) is an important part of zero-trust as well. MDM apps prohibit users from connecting any mobile devices to your network without meeting your network's security standards, enforce acceptable use policies for application access, and can even remotely wipe lost or stolen mobile devices.

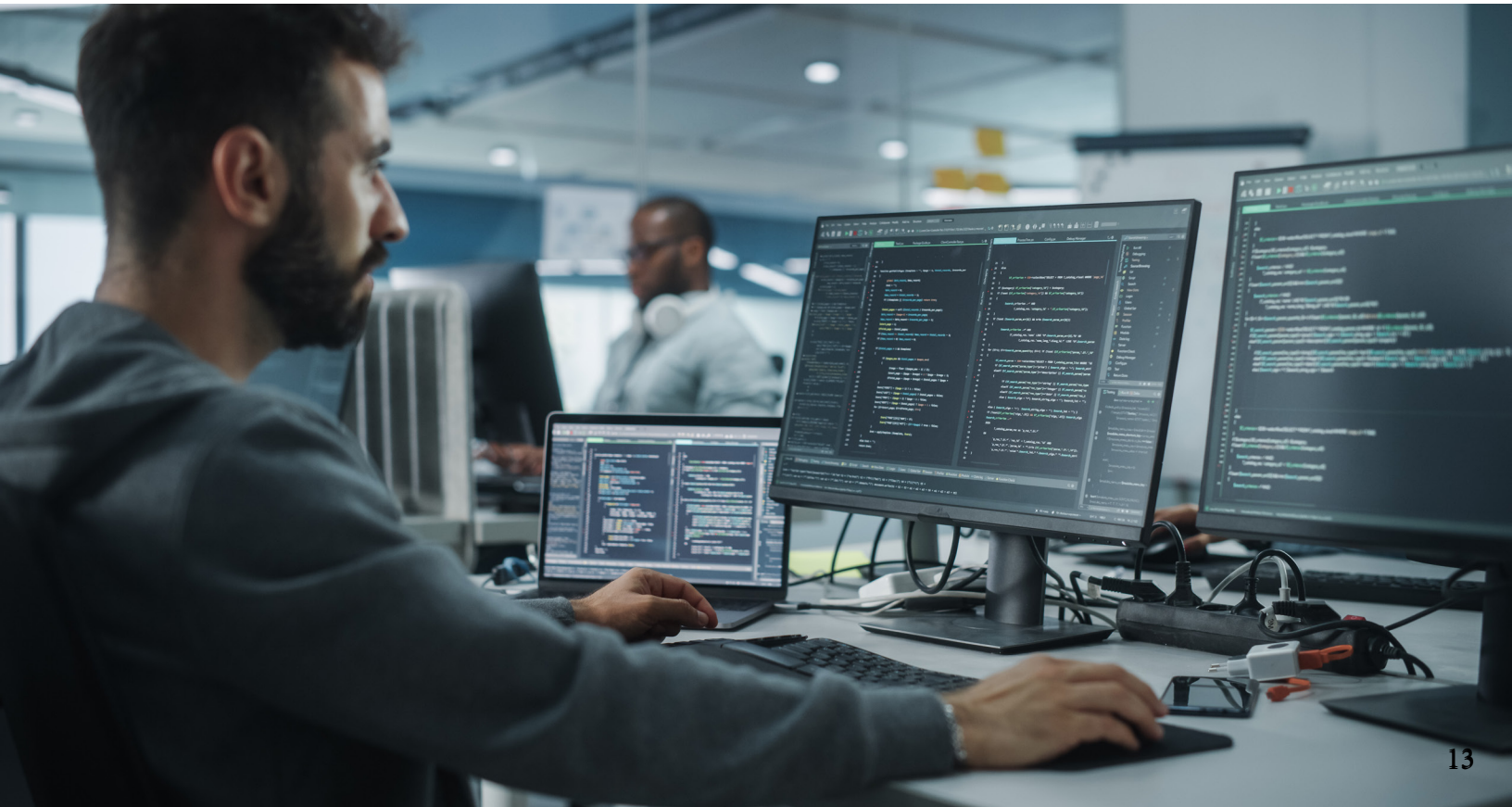
Create an incident response plan.

No matter how many slices there are in your Swiss cheese model, something can still get through in the rare case of all of the holes lining up. The sad reliability of cybersecurity is that no matter how much you minimize threats, your network will never be 100% impervious—so you should always have a clearly defined and outlined incident response plan in place for the 0.1% that get through.

Having a network security incident plan in place ahead of time means that if you do get hit, your entire organization can respond swiftly and effectively to limit the damage, close any vulnerabilities in your network, and get your organization back on track.

If applicable, maintain relevant regulatory security compliance standards.

Depending on your field and industry, the important regulatory security compliance standards you are already obligated to follow such as HIPAA in healthcare, PCI DSS in retail, or ISO standards are also building up your network security, so pay close attention to compliance audits to mitigate the possibility of internal threats.



It's Never Been More Important to Do Network Security Right

Cyber threats are a threat to every business and organization, regardless of size, and the threat of cyberattacks only seems to grow with every passing year. Taking everything into account to secure your network, especially if you manage a small IT team for a small company, might feel impossible given the manpower, budget, and resources at your disposal. Even large and well-equipped IT departments for big organizations can struggle to adequately secure their network.

It might seem impossible to do it all alone. It's a good thing, then, that you don't have to be.

Byteworks works to supplement your own IT team with professional expertise and streamline your organization's IT services with solutions that work for you, not against you. With proven experience helping organizations in the commercial and military world defend their critical assets, Byteworks will help you keep your people, data, infrastructure, and devices as secure as you need them to be.

When it comes to security, we offer robust and effective network and cybersecurity management services to help you augment the strength of your network, and backup and recovery services to get you back on your feet quickly in the event of a network security incident.

To schedule a meeting and learn how we can augment your IT department and help you build a solid and resilient security infrastructure.

CONTACT US